Cellebrite
ENDPOINT
INSPECTOR

Installation and Administration Guide

March 2022 | Version 1.3

Cellebrite

This page intentionally left blank.

Preface

This user guide address only the most recent version of Cellebrite Endpoint Inspector.

Legal Information

Typographic Conventions

This document uses these typographic conventions.

- The names of windows, views, tabs, dialog boxes, panes, panels, buttons, fields, options, checkboxes, and the like are in Initial Caps, or otherwise capitalized according to their labels.
- Keystrokes are shown in all capital letters, such as TAB, CTRL, OPT, CMD, SPACEBAR. Keys pressed at the same time are joined with +, such as CTRL+S, OPT+T.
- The names of elements that you are directed to interact with by clicking, selecting, or typing are shown in **bold**.
- Immediately contiguous menu actions such as clicking a toolbar button or menu, then immediately clicking another item in a resulting submenu, are separated with the > symbol, such as

  Edit > Copy

  Preferences > Data Collection

- *File names, folder names, file paths, disk names, drive names, volume names, partition names, and the like are shown in italic.* File extensions such as .pdf, .docx., .jpg, and so forth are not shown in italic.
- Variables are enclosed with <angle brackets>, such as <PLATFORM> VOLUMES, where <PLATFORM> is either MACOS or WINDOWS.
- `Anything you are directed to type exactly, such as file names, commands, or code, are shown in a console font.`

If you find any typos, inaccuracies, or other problems in this documentation, please send an email to support@cellebrite.com. Please include the title of the document, the version of the document, and the title of the topic in your message.

Contents

Document Revisions

This topic identifies information that is new, removed, or changed within this document since the previous version.

- This entire guide was revised to focus on audience and tasks, and to integrate information about mobile collections.
- What's New in Version 1.3 is a new topic.

What's New in Version 1.3

These features are new in this version of Endpoint Inspector. Information in this chapter supersedes the remainder of this document.

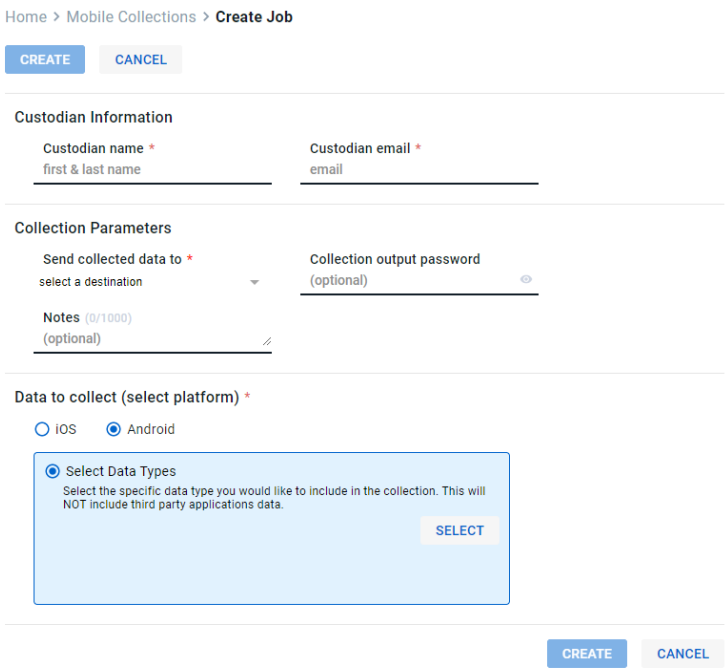
The Endpoint Inspector web interface is supported on these web browsers:

- Chrome
- Edge
- Firefox
- Safari

These features are new in this version of the Endpoint Inspector web interface:

Collect Data from Android Mobile Devices

On the Mobile Collections page in the Endpoint Inspector web interface, examiners can now create and manage collections for Android mobile devices. The same mobile agent supports collecting from both iOS and Android.



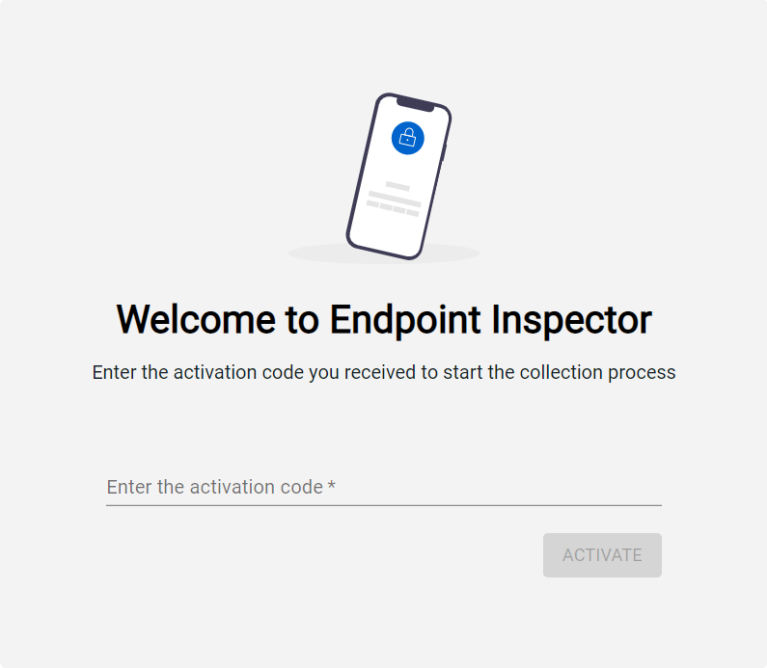
When you create a mobile collection job, you can select Android as the platform and then select data types to collect. On the Select dialog box, you can select all data or you can mark any or all of these other checkboxes:

- Select All
- Archives
- Audio
- Calendar
- Call Logs
- Contacts
- Documents
- MMS
- Pictures
- SMS
- Videos

Note: Data cannot be collected from third-party applications or cloud-based applications at this time. Data can be collected only from the device itself.

The examiner sends the activation token and URL for downloading the mobile agent to the person with custody of the Android device.

The custodian downloads and installs the mobile agent onto their computer. The computer must be restarted to complete the installation. After the computer is restarted, the custodian finds the installed *CellebriteMobileAgent* on their desktop and runs it. The Welcome to Endpoint Inspector page opens in the custodian's default web browser.



Just as with collections from iOS devices, the custodian then enters the activation token provided to them by the examiner. Instructions on the Endpoint Inspector web interface guide the custodian in the process of preparing and connecting their Android device and alerts that an agent will also be automatically installed on the Android device. This device agent is required to collect the data.

The data collection is transferred to the custodian's computer, where the agent creates a .zip file and then sends it to the specified storage repository. The .zip file may be password protected if the examiner defined the mobile collection job to require a collection output password. The device agent removes itself after the collection process is complete. If the device agent fails to remove itself, instructions within it show the custodian how to manually remove it.

Support for Amazon S3 Buckets

There are now three destination types for both computer and remote mobile collection jobs. In addition to Network Share and SFTP paths, you can set up an Amazon S3 bucket as a destination. This includes GovCloud.

You must use web pages provided by Amazon to create the bucket.

1. Use the AWS Management Console to specify the name and region where the bucket will be hosted.
2. Use the IAM dashboard to create a role and policies for the bucket.
3. Create a user and attach policies to the user.

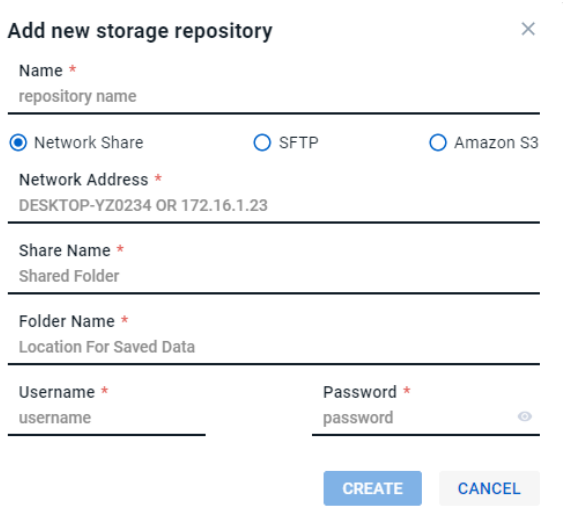
Note: Keep those Amazon web pages open to refer to while you create the Amazon S3 storage repository in the Endpoint Inspector web interface. For more information, see Set Up an Amazon S3 Storage Repository.

Support for Multiple Storage Destinations

On the Settings page, you can now create and manage multiple storage repositories. These repositories can serve as destinations for both computer and remote mobile collection jobs.

Create a Storage Repository

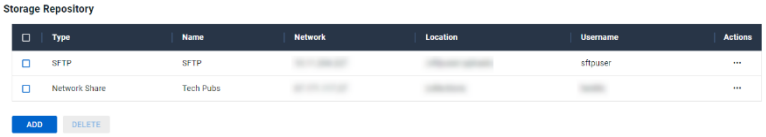
1. Log in to the Endpoint Inspector web interface and then click **Settings**.
2. Click **ADD** under Storage Repository.
   The Add new storage repository dialog box appears.



3. In the **Name** field, type the name for this storage repository.
4. Select the appropriate type of destination and then complete the remaining fields.

Manage Storage Repositories

1. Log in to the Endpoint Inspector web interface and then click **Settings**.
2. Under **Storage Repository**, you can see a list of all the storage repositories created in this Endpoint server.

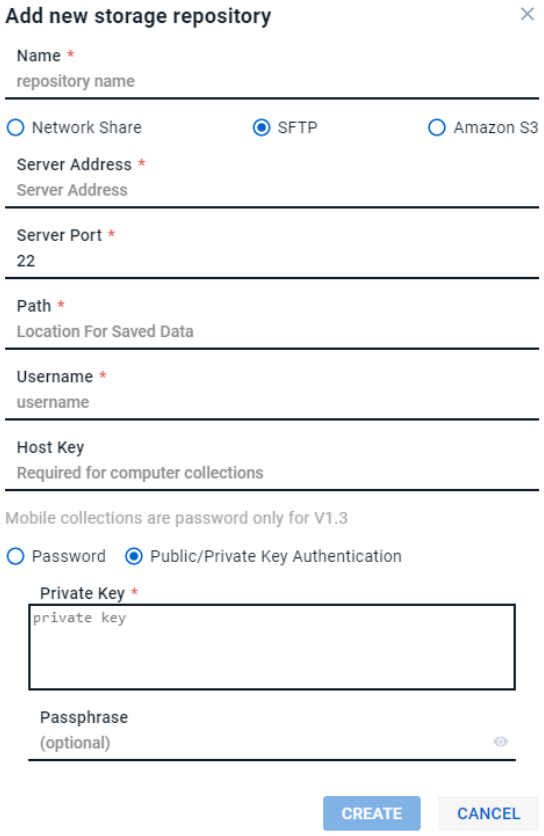


3. Choose the appropriate action.

Action	Steps
Edit a repository	a. For the appropriate repository, click **Actions** and then click **Edit Storage Repository**. b. In the Update storage repository dialog box, change the appropriate information and then click **Update**.
Delete a repository	Mark the checkbox for the appropriate repository and then click **Delete**.

SFTP Public/Private Key Authentication for a Storage Repository

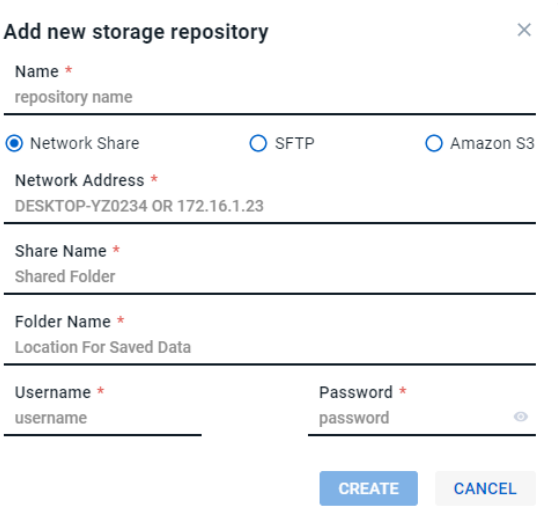
For SFTP repositories, you can now set up public or private key authentication.



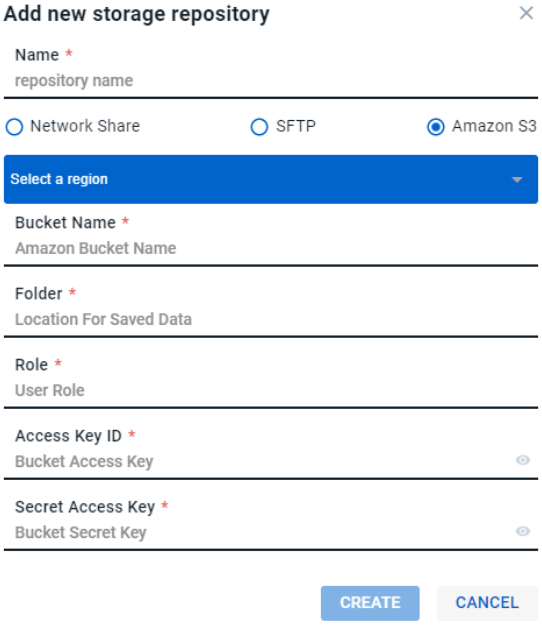
Set Up an Amazon S3 Storage Repository

After you have created the Amazon S3 bucket, keep those web pages open so you can refer to them when you create the storage repository in the Endpoint Inspector web interface.

1. Log in to the Endpoint Inspector web interface and then click **Settings**.
2. Click **ADD** under Storage Repository.
   The Add new storage repository dialog box appears.



3. In the **Name** field, type the name for this storage repository.
4. Click **Amazon S3**.



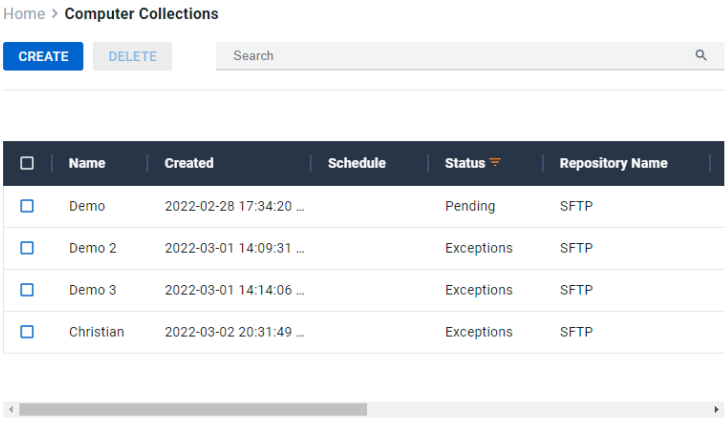
5. Click **Select a region** and then select the region that matches the one you selected for the bucket you created in the AWS Management Console.

6. Type appropriate information in these fields.

Field	Description
Bucket Name	The name of the bucket just as it was defined in the AWS Management Console
Folder	The name of the folder within the bucket that will store collected data sets
Role	The name of the role that lets a user get and put objects for the bucket, as defined in the AWS Management Console
Access Key ID	The access key ID for the AWS user account
Secret Access Key	The secret access key ID for the AWS user account

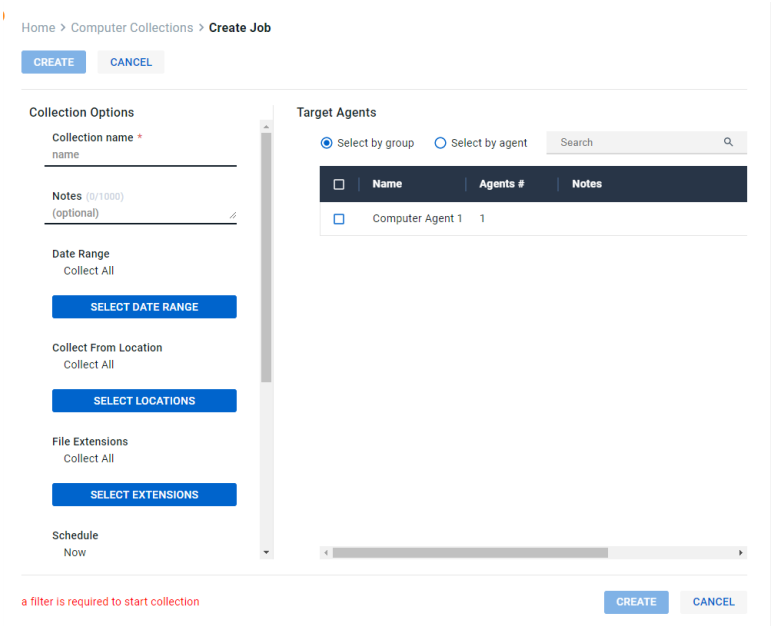
Schedule Collections from Remote Computers,

On the new Computer Collections page in the Endpoint Inspector web interface, examiners can create, monitor, and manage computer collection jobs.



The Status column shows Exceptions when a computer collection job fails. A job will fail if there is not enough available space on the remote computer to permit data collection or if the connection between the remote computer and the storage repository is lost.

On the Create Job dialog box, you must provide a name for the computer collection job and then set filters for the data to be collected. You can also provide notes for the collection job.



Under Collection Options, these are the filters you can set.

Filter	Description
Date Range	You can choose any of these options or set a custom date range: • Today • Yesterday • Last 7 days • Last 30 days • This Month • Last Month • Last Year
Folders	You can select all folders, select any of the pre-set folders, or specify custom folders. These are the pre-set folders: • All users – Folders • All users – Desktop items • All uses – Documents • All users – Pictures • All users – Downloaded items • Event Logs • iOS backups • iCloud data • Unified Logs • Shell data To specify custom folders, you can type drive letters and file paths. Use an asterisk (*) as a wildcard. Use a comma to separate multiple locations.
File Extensions	You can select all, select any of the pre-set categories, or specify custom file extensions. Use a comma to separate multiple custom file extensions. These are the pre-set categories: • Text Files • Data Files • Audio Files • Video Files • 3D Image Files • Image Files • Vector Image Files • Page Layout Files • Spreadsheet Files • Database Files • Executable Files • Game Files • CAD Files • GIS Files • Web Files • Plugin Files • Font Files • System Files • Settings Files • Encoded Files • Compressed Files • Disk Image Files • Developer Files • Backup Files • Misc Files
Schedule	You can set the collection job to run now, select a date and a time (any half hour between 00:00 and 23:30), or specify a custom date. These are the dates you can select: • Today • Tomorrow • In 5 days • In 1 week • In 2 weeks
Volatile Collection	You can choose whether to collect volatile artifacts. For more information, see Collect Volatile Artifacts from Remote Computers.

Note: You can only specify what to include in the collection; you cannot set exclusions.

You must also select a destination where the data collection will be sent.

Under Target Agents, you can choose one or several agents to collect from, or you can choose one or several groups to collect from.

You may edit collection jobs that are in a Pending status.

Collect Volatile Artifacts from Remote Computers

To improve support for incident response, you can now choose to collect artifacts from running remote Windows computers.

When an examiner creates a collection job on the Computer Collections page, they can specify that volatile artifacts should be collected. A single toggle targets these categories of artifacts for Windows computers.

Category	Description
Processes and modules	The names and file handles of all running processes and modules.
Network data	List of adapters and related statistics and tables. Information about network shares.
Clipboard data	Lists all the content of the computer's clipboard.
Open files	Lists all open files on the computer by process.
Desktop	Provides a screen capture of the computer desktop.

Link to Web Page Announcing New or Changed Features

If the Endpoint Inspector web interface was updated after you last logged in, a web page appears that provides information about new and changed features.

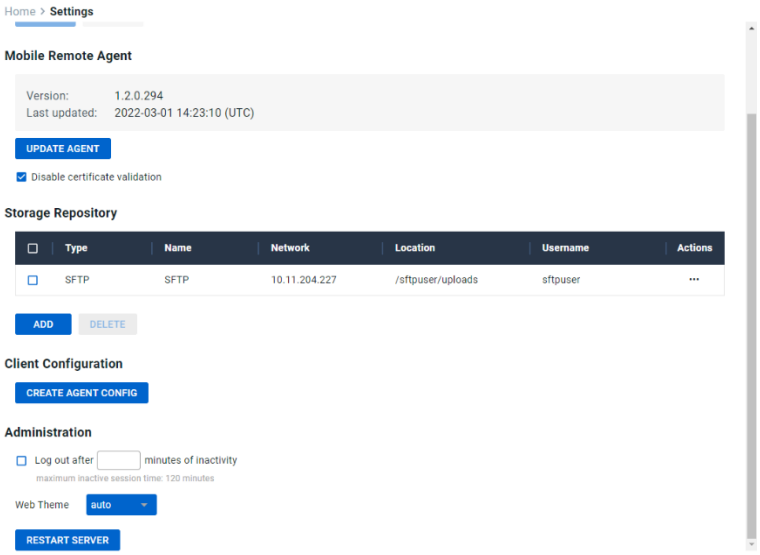
If the Endpoint server does not have an internet connection, a QR code appears instead. You can scan this QR code with your mobile phone or use it on a different computer to see this web page.

You can open this web page any time by clicking the menu button in the upper right corner of the Endpoint Inspector web interface and then clicking **About V<version number>**.

New Settings

Under Administration at the bottom of the Settings page, you can now choose whether users in the Endpoint Inspector web interface are logged out after inactivity and set the number of minutes of inactivity up to 120.

You can also specify whether the Web Theme is automatic, light, or dark.



Introduction

Cellebrite Endpoint Inspector allows an organization to create logical data collections from remote computers and mobile devices without shipping any hardware. Examiners do need to use Cellebrite Inspector.

The Endpoint server is installed on a single Windows computer. Servers for Endpoint Inspector are not aware of each other. Administrators must use a web browser to log in to the server to manage it as well as to manage agents and users.

The Endpoint agent enables data to be collected from remote Windows and Mac computers. Collection over a VPN is supported. The installation packages for the Endpoint agent can be distributed, installed, and configured on the remote computers with standard management tools. An installation wizard is present for users of remote computers who must manually install the Endpoint agent.

With the participation of the person in custody of a mobile device, data can be collected and sent to a physically distant location for storage and examination. The only components that must be in physical proximity are the mobile device and the custodian's computer, which must be connected with an appropriate USB cable during collection.

Examiners access Endpoint Inspector through Cellebrite Inspector running on their own computers. Examiners are logged in and granted their license for each session through the Endpoint server.

Within Cellebrite Inspector, examiners can connect to the Endpoint agents assigned to them. CPU resources may be consumed from both the examiner's computer and the remote computer, and in rare cases from the Endpoint server as well. Once connected, examiners can collect and analyze data from the corresponding remote computers when they are online and connected to the network. Examiners can use these views for selecting data to collect.

- Browser
- File Filter
- Thumbnails

Examiners can also request a file from the endpoint computer to see file data in the Hex view, Strings view, and Preview tabs.

Examiners save the selected files into a collection file with the Logical Evidence file format (L01). This format is widely supported by forensic and eDiscovery tools, and preserves file content, metadata, and folder structure. These L01 files are ingested into Cellebrite Inspector, where analysts can use robust analysis and reporting tools.

Each license provides one server for Endpoint Inspector. One server can support up to 1000 agents installed on endpoints, up to ten concurrent connections to those endpoints, and up to three examiners.

Remote Mobile Collection

Each mobile license is term based and defines the quantity of mobile collection jobs your organization can consume. In this way, each license represents a pool of available mobile collection jobs. When a license term expires, you can no longer create mobile collection jobs.

When a mobile collection job is created, it is consumed and removed from the pool. A collection job cannot be created if all available jobs have been consumed from the pool.

When a mobile collection job saves data, it is permanently consumed and removed from the pool. This is true even if the collected data is not successfully transmitted to the location designated by the examiner, either automatically or manually.

Each mobile collection job can be run only once; however, if a collection job does not complete successfully, the custodian can restart it.

You can delete a mobile collection job before the custodian starts the collection. Deleted collection jobs are returned to the pool.

If a mobile collection job fails with no data saved to the custodian's computer, it can be deleted and returned to the pool.

File Format for Remote Mobile Collection

Collected data is saved in UFED zip format. This format can be ingested and examined with Inspector 10.4.1 and later or with Physical Analyzer 7.47 and later. These UFED zip files can be password protected.

Data Types Supported for Remote Mobile Collection

These types of data may be collected from iOS devices, ingested, parsed, and examined by Endpoint Inspector or Physical Analyzer.

Applications native to the iOS platform can collect these types of data.

- Advertising ID
- Audio
- Browser Data
- Calendar
- Call Logs
- Contacts
- IM
- Pictures
- SMS/MMS
- Videos

Depending on the specific version in use, some data can be collected from these third-party applications.

- WhatsApp
- WeChat
- Facebook messenger

Deleted Data

For supported applications, the full database may be recovered. Any deleted messages or threads that are found are presented. Deleted files such as images, documents, and full database files cannot be recovered.

Definition of Terms

Term	Definition
agent	Software that collects data from a remote computer.
case	Data collections ingested into Inspector are examined within the context of a case. A case may contain multiple data collections.
computer collection job	These are created by the examiner in the Endpoint server web interface to specify what data to collect from a remote computer, and to schedule the date and time when collection should start. A collection job also specifies the destination of the collection and the password required to access the collection during examination.
custodian	The person with custody and control of a mobile device. The custodian participates in collecting data from the mobile device.
device agent	Software that assists in collecting data from an Android mobile device.
examiner	The person who uses the Endpoint server web interface to create, monitor, and manage collection jobs. This person must be assigned the Analyst role. This person also examines the collected data using either Inspector or Physical Analyzer.
mobile agent	Software that collects data from a mobile device.
mobile collection job	These are created by the examiner in the Endpoint server web interface to specify what data to collect and—by specifying the custodian—which mobile device to collect it from. A collection job also specifies the destination of the collection and the password required to access the collection during examination.
remote collection	The process or result of collecting data from a remote computer and sending it to a physically distant location for storage and examination.
remote mobile collection	The process or result of collecting data from a remote mobile device and sending it to a physically distant location for storage and examination. This process requires the participation of the person with custody of the mobile device. The only components that must be in physical proximity are the mobile device and the custodian's computer, which must be connected with an appropriate USB cable during collection.

System Components and Requirements

These are the system components and requirements required to run Endpoint Inspector, to create and transmit collections from remote computers and mobile devices, and to ingest, parse, and examine the collected data.

Component and Definition	System Requirements
Endpoint server Manages licenses and authentication. Used by examiners to create and monitor collection jobs.	• Windows 10 1909 or newer • Windows Server 2019 or newer • 200 GB available disk space • Minimum 16 GB RAM • Minimum 4 CPU
Endpoint agent Installed on the custodian's computer. Receives the data collection from the mobile agent and sends it to the destination specified by the examiner.	• Windows 10 1909 or newer • macOS 10.14, 10.15, and 11.6 (Intel)
Endpoint mobile agent Automatically downloaded and installed on a custodian's computer for each collection. Collects data from the connected mobile device and sends it to the destination specified in the collection job. **Note**: Data can be collected only from iOS devices.	Windows 10 1909 or newer
Device agent Required only for collection from Android devices. Automatically downloaded and installed on the Android device for each collection. Automatically removed from the device when collection is complete.	Android platform
Endpoint Inspector 10.4.1 and later Used by examiners to ingest, parse, and analyze collected data within the context of a case.	• Windows 10 1909 or newer • Inspector is supported on Mac OS X 10.12.6 or newer, therefore Endpoint Inspector may work as well. For more information, see the "Hardware and Software Requirements" topic in the *Cellebrite Inspector User Guide*.
Physical Analyzer 7.47 and later Used by examiners to ingest, parse, and examine collected data.	For information about Physical Analyzer, see the *Cellebrite Physical Analyzer User Manual*.

Default Server Ports

Port	Port Numbers
Web Configuration Port	443
Authentication Port	20001
Agent Communication Port	20002
Agent Direct Connect Port	20003

Getting Support

You can log in to MyCellebrite portal at https://community.cellebrite.com, which provides access to resources and support.

- Keep your products updated.
- Contact Support or review the knowledgebase.
- Download user manuals and data sheets.
- Manage your product licenses.
- Get expert assistance.

You can also send an email to technical support at support@cellebrite.com.

These technical publications are available for download.

- *Cellebrite Endpoint Inspector 1.3 Release Notes*
- *Cellebrite Endpoint Inspector 1.3 Communications and Security Guide*
- *Cellebrite Inspector User Guide for Endpoint Inspector 1.3*
- *Cellebrite Inspector 10.5 Quick Start Guide*
- *Cellebrite Inspector 10.5 Portable Case Guide*

Known Issue

This is a known issue related to remote mobile collection.

When a computer has UFED installed on it and then the Endpoint Inspector mobile agent is installed and later uninstalled, drivers are also removed from that computer. The result is that UFED no longer works. To resolve this, you can uninstall and reinstall UFED.

Installation and Deployment

The server for Endpoint Inspector must be installed on a Windows computer. This computer can be physical or virtual. For more information, see System Components and Requirements.

After installation, you can activate the license and create the first administrator account. Then you can use the first administrator account to complete the remaining installation and deployment tasks. This may include creating additional administrator accounts.

Refer to the Installation and Deployment Checklists to ensure the tasks are completed in the required order. These checklists provide links to topics to support you in completing these tasks.

For various reasons, the required tasks may differ between a test deployment and a production deployment.

Before you begin: You should understand the Security Certificate set of topics.

Installation and Deployment Checklists

You should use these checklists to ensure installation and deployment tasks are performed in the correct order to properly install components for Endpoint Inspector and to verify that data can be collected. Some tasks may be optional depending on whether you are deploying for test purpose or for production.

Before you begin: You should review the checklists to be sure you understand the differences between test and production deployments.

Endpoint Server and Agent

	Task	Supporting Topics
☐	Install the Endpoint server.	Install and Configure the Endpoint Server
☐	In the Endpoint Inspector web interface, define ports and the server address.	Update Ports and Server Address Restart the Endpoint Server
☐	If it is necessary for testing, in the Endpoint Inspector web interface, disable security certificate validation.	Disable Certificate Validation During Testing
☐	If it is necessary for production, replace the security certificate.	Replace the Security Certificate
☐	In the Endpoint Inspector web interface, define settings the agent and then save the agent configuration file.	Create and Export an Agent Configuration File

	Task	Supporting Topics
☐	For testing, manually install the agents and the *config.json* file on the few computers that will be used to test remote computer collections. Get the agents and the *config.json* file from the Settings page in the Endpoint Inspector web interface.	
☐	For production, install the agents and the *config.json* file on your organization's remote Mac and Windows computers,	Deploying the Endpoint Agent to Mac Computers with JAMF Deploying the Endpoint Agent to Windows Computers with Unattended Installation
☐	Note: For testing, it is easiest to manually install the agents and the *config.json* file on the few computers that be used to test remote computer collections.	
☐	In the Endpoint Inspector web interface, create users. Note: For testing, you only need to create a few users.	Manage Users
☐	In the Endpoint Inspector web interface, create groups for agents and assign users to groups. Note: For testing, you only need to create a few groups.	Manage Agents and Groups
☐	In the Endpoint Inspector web interface, verify that the agents installed on the remote computers are listed, and then assign the agents to the appropriate group.	Manage Agents and Groups
☐	On an examiner's computer with Inspector installed, verify that Inspector can connect to the Endpoint server, list agents assigned to the examiner, and start browsing the file system for a selected agent.	See the *Cellebrite Endpoint Inspector User Guide*.

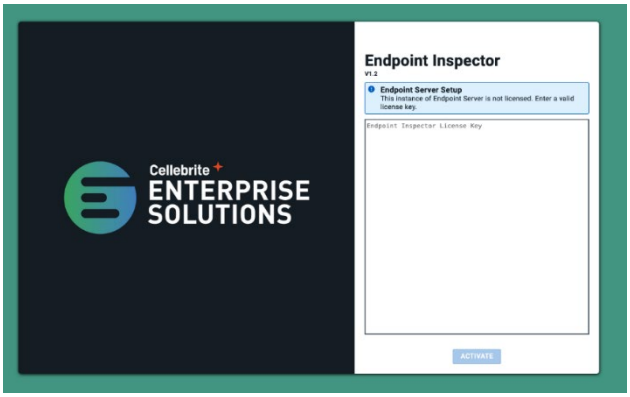
Remote Mobile Collection

	Task	Related Topics
☐	In the Endpoint Inspector web interface, add the mobile license.	Add a Mobile Collection License
☐	In the Endpoint Inspector web interface, update the mobile agent.	Update the Mobile Agent
☐	In the Endpoint Inspector web interface, set the default destination for collections.	Set the Default Destination for Mobile Data Collections
☐	In the Endpoint Inspector web interface, create a collection job.	Create a Mobile Collection Job
☐	Send the activation token and the link to download the mobile agent to the intended custodian.	
☐	On the custodian's computer, download and install the mobile agent, restart the computer, run the mobile agent, and then enter the activation token to begin collecting data.	Create and Send a Mobile Collection
☐	In the Endpoint Inspector web interface, verify that the mobile agent's activity is visible. Also verify that the mobile collection file is saved to the appropriate location.	Monitor, Find, and Select Mobile Collection Jobs
☐	On an examiner's computer with Inspector installed, verify that Inspector can ingest the mobile collection file.	See the *Cellebrite Endpoint Inspector User Guide*.

Install and Configure the Endpoint Server

Note: Be sure the Windows computer meets the system requirements. For more information, see System Components and Requirements.

1. On the appropriate computer, run the installer for the Endpoint server, then follow the prompts in the Setup wizard.
2. In a web browser, go to https://localhost.
3. On the security warning page for your web browser, proceed to the Endpoint server.
   The Endpoint Server Setup page appears.



4. Paste the license key into the text box, and then click **ACTIVATE.**
   The Server Address field shows the IP address of the Endpoint server.
5. Click **CONTINUE**.
6. Select the appropriate connection method for the Postgres Database.
   - **User Internal Database**, and then click **CONTINUE**.
   - **Use External Database**, and then provide values for these fields.
     a. Address
     b. Port
     c. Database
     d. Username
     e. Password
     f. SSL Mode
7. Under Administrator Account, type the username and password to create the primary administrator account for this server, and then click **CONTINUE**.
   The login page for Endpoint Inspector appears with credentials prefilled for the primary administrator account you just created.
8. Click **LOG IN**.

The server for Endpoint Inspector is installed, licensed, and you are logged in to the server as the first administrator. Now you can set up Endpoint Inspector and deploy agents. For more information, see these topics:

- Security Certificate
- Managing Settings

Security Certificate

When you deploy Endpoint Inspector for testing purposes, you may not need to test validation for the mobile agent network authentication security certificate. For this reason, you can choose to bypass security certificate validation for mobile agent network authentication. For more information, see Disable Certificate Validation.

Production Considerations

When you deploy Endpoint Inspector for production purposes, decide which of these options best suits your organization.

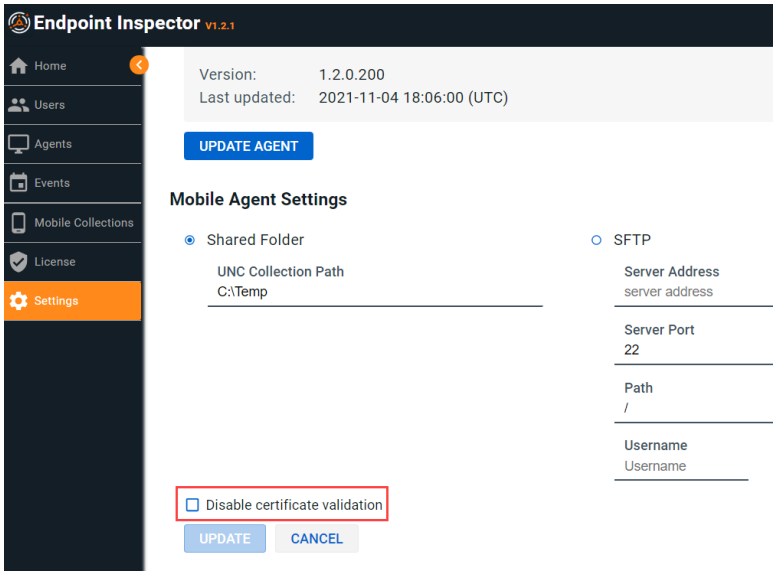
- If your organization issues its own certificates (either private PKI or through a private certificate authority), you should install your own certificate for mobile agent network authentication on the Endpoint server. For more information, see Replace the Security Certificate. You should also ensure that certificate validation is not disabled. For more information, see Disable Certificate Validation.
- If your organization does not issue its own certificates, you should partner with a commercial trusted certificate authority (such as Digicert, Entrust Datacard, Globalsign, GoDaddy, Sectigo, and so forth) and be provisioned accordingly. For more information, see Replace the Security Certificate. You should also ensure that certificate validation is not disabled. For more information, see Disable Certificate Validation.
- If your organization does not mandate the full security stack of benefits derived from using a private PKI or commercial certificate authority, you may continue to use the default self-signed certificate.

Note: The **Server Address** field under Mobile Remote Agent on the Settings page must match the certificate-assigned DNS address.

Disable Certificate Validation During Testing

You may choose to disable validation for the mobile agent network authentication security certificate. This may be appropriate when you are testing Endpoint Inspector remote mobile collection but do not need to test certificate validation. For more information, see Security Certificate.

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **Settings**.
3. Scroll down to the **Mobile Agent Settings** section.



4. Mark the checkbox labeled **Disable certificate validation**.

After your testing is complete, if your organization will continue to use this Endpoint server for production, you should install a certificate provided by a commercial trusted certificate authority or your own private PKI certificate and ensure that this checkbox is cleared to enable mobile agent certificate validation. For more information, see Production Considerations and Replace the Security Certificate.

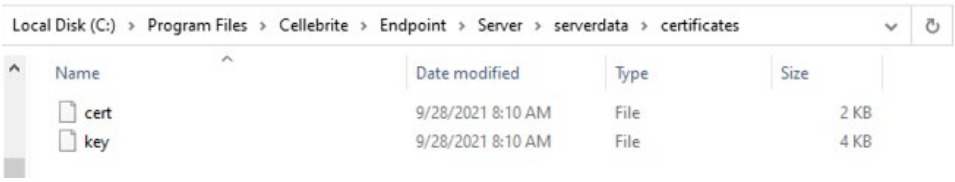
Replace the Security Certificate

You must place these files for the new mobile agent network security certificate in a specific folder on the Endpoint server.

- cert
- key

It's a good idea to back up the existing certificate files in case you need them later.

1. On the computer that is the Endpoint server, open a File Explorer window and navigate to this folder.
   %PROGRAMFILES%\Cellebrite\Endpoint\Server\serverdata\certificates



2. For backup purposes, rename the existing *cert* and *key* files and move them to an appropriate backup location.
3. Copy the *cert* and *key* files for the new certificate into the folder described in Step 1.
4. Restart the server.
5. Log in to the Endpoint Inspector web interface and on the Settings page, unmark the checkbox labeled **Disable certificate validation**.

Deploying Endpoint Agents

This section addresses whole-enterprise deployment for production purposes. This is not necessary for testing purposes within your environment.

Endpoint agents must be installed on the remote Windows or Mac computers before data can be collected from them with Endpoint Inspector.

There are separate installation packages for the Endpoint agents on the Windows and Mac platforms.

The installation packages for the Endpoint agent can be distributed, installed, and configured on remote computers with standard management tools. You must create and distribute the agent configuration file along with the installation file. There is an installation wizard for users of remote computers who must manually install the Endpoint agent.

An Endpoint is defined when its agent first connects successfully to the Endpoint server.

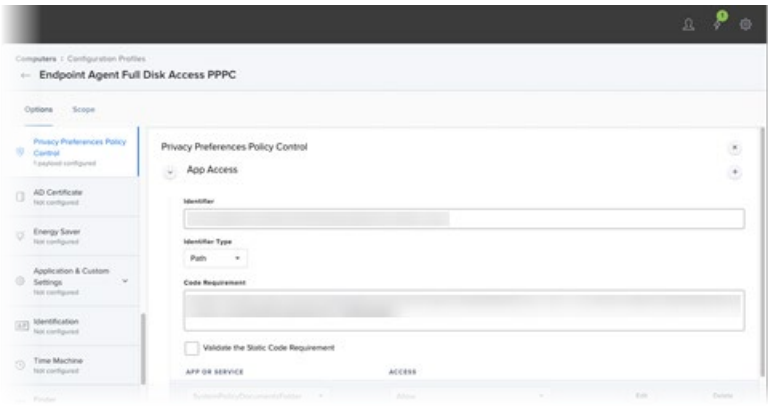
Deploying the Endpoint Agent to Mac Computers with JAMF

This task assumes familiarity with JAMF. For more information, see https://www.jamf.com/.

First, you must configure the Privacy Preferences Policy Control for full disk access. Then you can create a policy to deploy and install the Endpoint agent.

Configure Privacy Preferences Policy Control

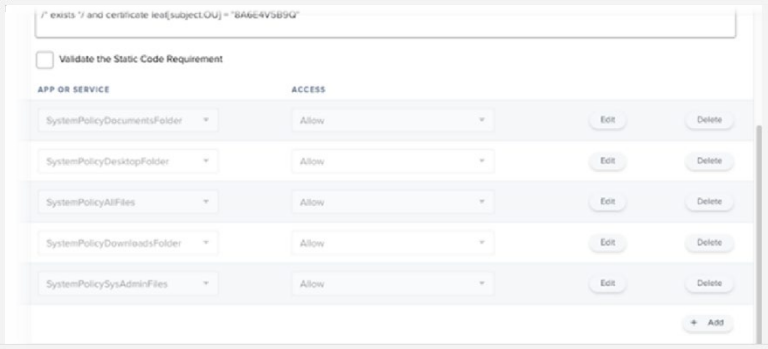
You can use JAMF to create a new configuration profile to grant full disk access to the Endpoint agent.



1. In JAMF, create a new configuration profile and add these entries to the Privacy Preferences Policy Control setting.

Field	Value
Identifier	`/Library/Application Support/Cellebrite/Endpoint/Agent/bin/Cellebrite_Endpoint_Agent`
Identifier Type	`Path`
Code Requirement	`identifier "Cellebrite_Endpoint_Agent" and anchor apple generic and certificate1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists*/ and certificate leaf[subject.OU] = "8A6E4V5B9Q"`

2. Enable the appropriate disk and folder access levels for the Endpoint agent.

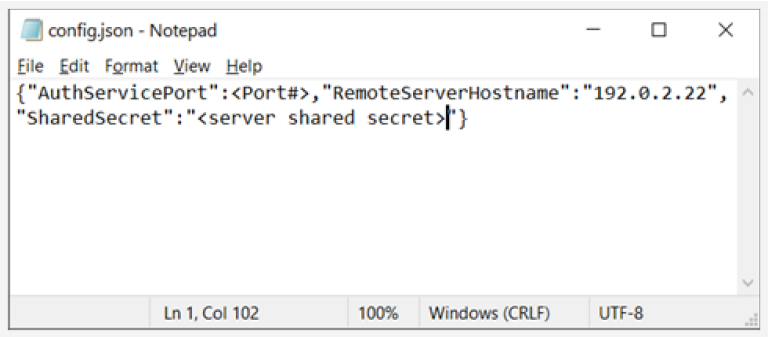


App or Service	Access
SystemPolicyDocumentsFolder	Allow
SystemPolicyDesktopFolder	Allow
SystemPolicyAllFiles	Allow
SystemPolicyDownloadsFolder	Allow
SystemPolicySysAdminFiles	Allow

Create a Policy to Deploy and Install the Endpoint Agent

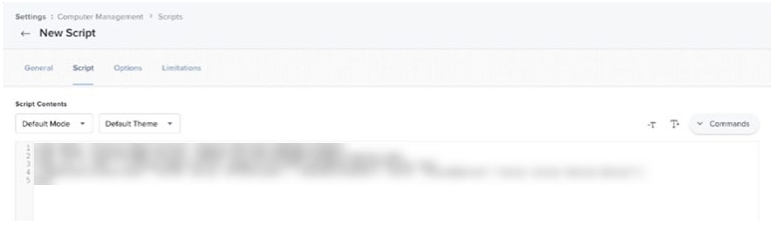
You can use JAMF to create a policy to deploy and install the Endpoint agent. The configuration profile must be deployed before the installer package.

Note: In the server for the Endpoint server, export the *config.json* file from the Settings page. For more information, see Create and Export an Agent Configuration File. Refer to this file for the hostname or IP address, Authentication Port, and shared secret for this Endpoint server. This is an example of a *config.json* file with placeholder text enclosed within angle brackets and an example IP address.

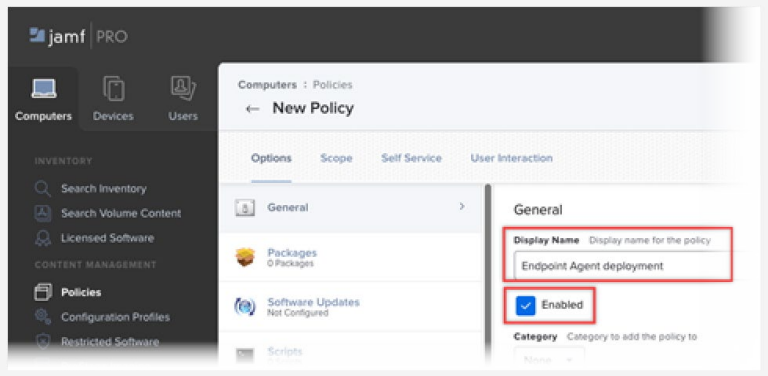


1. In JAMF, under Computer Management settings, upload the Endpoint Agent Config installer package to your distribution repository.
2. Create a JAMF script to create the necessary folder, to create the *config.json* file within that folder, and to populate that file as required.
   Example:

```
sudo mkdir /Library/Application\ Support/Cellebrite/Endpoint
sudo mkdir /Library/Application\ Support/Cellebrite/Endpoint/Agent
sudo mkdir /Library/Application\ Support/Cellebrite/Endpoint/Agent/bin
sudo mkdir /Library/Application\ Support/Cellebrite/Endpoint/Agent/bin/agentdata
sudo touch /Library/Application\ Support/Cellebrite/Endpoint/Agent/bin/agentdata/config.json
sudo cat << EOF > /Library/Application\ Support/Cellebrite/Endpoint/Agent/bin/agentdata/config.json
{"RemoteServerHostname":"<server IP address or hostname>", "AuthServicePort": <Authentication Port>,
"SharedSecret":"<server shared secret>"}
EOF
```

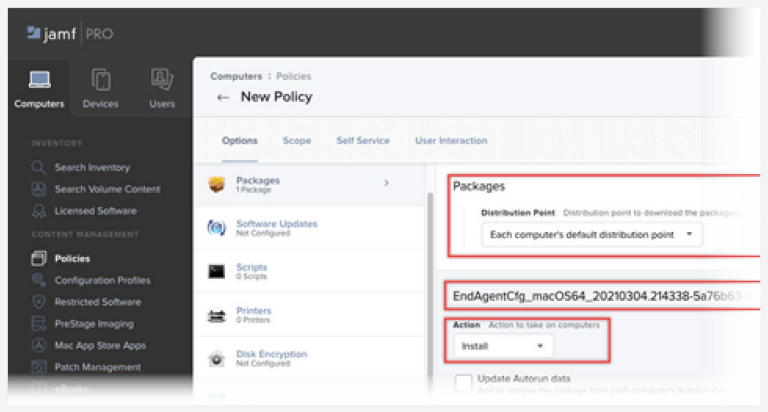


3. Create a policy to deploy the installer package and the *config.json* file to the appropriate Mac computers, with the script configured to run before the package install.
    a. On the General page, provide a **Display Name** such as Endpoint Agent deployment
    b. Mark the **Enabled** checkbox.



4. On the Packages page, make these entries.
    a. Set the **Distribution Point** to `Each computer's default distribution point`.
    b. Add the installer package for the Endpoint agent.
    c. Set the **Action** field to `Install`.
5. On the Scripts page, set the **Priority** for the Endpoint agent script to `Before`.

Now you can deploy the configuration profile and installer package to each target Mac computer.



Deploying the Endpoint Agent to Windows Computers with Unattended Installation

These examples use PowerShell and the command line to deploy the Endpoint agent to Windows computers with unattended installation. All required fields are available in the *config.json* file saved from the Endpoint server.

MSI Installer accepts standard arguments and then expects Wrapped Arguments for the wrapped installer.

The Endpoint Agent Service does not start automatically from an unattended installation.

This syntax is required.

```
WRAPPED_ARGUMENTS="/VERYSILENT /ip=server_address /port=20001 /secret=supersecretfromconfigjson"
```

Command Prompt Code Example

```
msiexec /i "location_to_msi" /qn /norestart WRAPPED_ARGUMENTS="/VERYSILENT /ip=server_address
/port=20001 /secret=supersecretfromconfigjson"

net start "Endpoint Agent"
```

PowerShell Code Example #1

This example is for a silent install with Wrapped Arguments hard coded, followed by starting the Endpoint Agent Service.

```
$localfile = "location_to_msi"

$servicename = "Endpoint Agent"

$MSIArguments = @(

          "/i"

          ('"{0}"' -f $localfile)

          "/qn"

          "/norestart"

          'WRAPPED_ARGUMENTS="/VERYSILENT /ip=server_address /port=20001 /secret=supersecretfromconfigjson"'

)

Start-Process "msiexec.exe" -ArgumentList $MSIArguments -Wait -NoNewWindow

Start-Service $servicename
```

PowerShell Code Example #2

This example is for a silent install with Wrapped Arguments parsed from *config.json*, followed by starting the Endpoint Agent Service.

```
$localfile = "location_to_msi"
$servicename = "Endpoint Agent"
$configparsejson = "location_to_config.json | ConvertFrom-Json

$ip = $configparsejson.RemoteServerHostname
$port = $configparsejson.AuthServicePort
$secret = $configparsejson.SharedSecret
$wrapped = ('WRAPPED_ARGUMENTS="/VERYSILENT /ip={0} /port={1} /secret={2}"' -f $ip, $port, $secret)

$MSIArguments = @(
    "/i"
    ('"{0}"' -f $localfile)
    "/qn"
    "/norestart"
    "$wrapped"
)

Start-Process "msiexec.exe" -ArgumentList $MSIArguments -Wait -NoNewWindow
Start-Service $servicename
```

Administrator Tasks

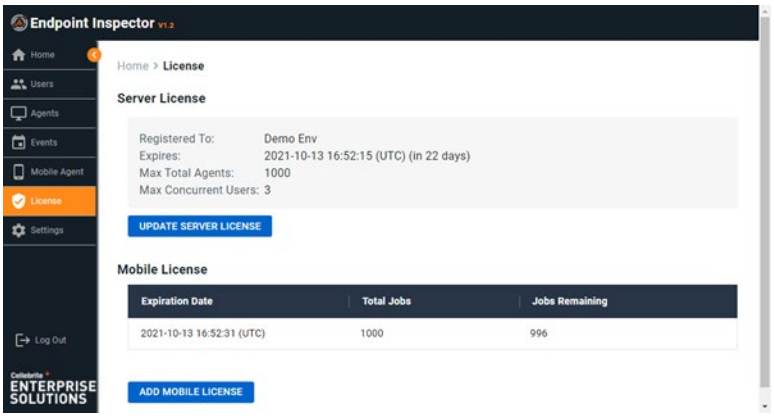
These topics describe tasks that administrators complete to deploy Endpoint Inspector and also in the course of normal operations.

Managing Licenses

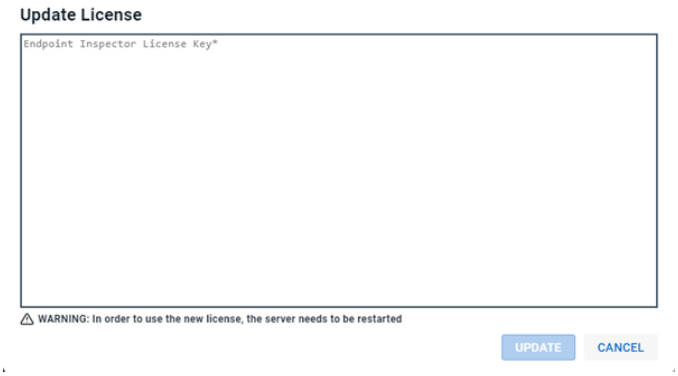
Administrators can complete these tasks on the Licenses page in the Endpoint server web interface.

Update the Endpoint Server License

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **Licenses**.
   The Licenses page appears.



3. Under **Server License**, click **UPDATE SERVER LICENSE**.
   The Update License page appears.

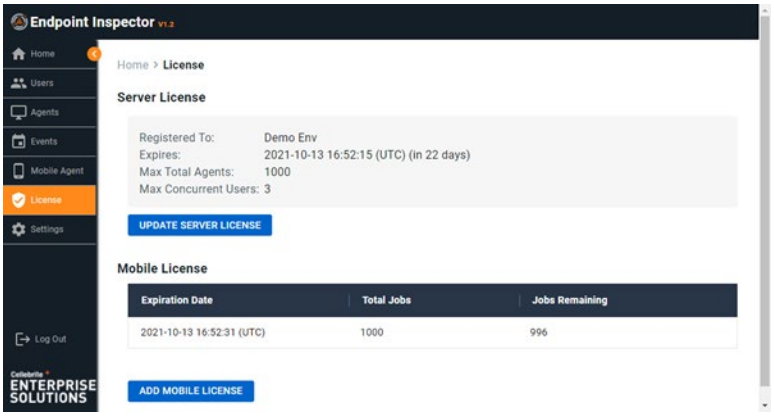


4. Paste the license into the text box and then click **UPDATE**
5. Restart the Endpoint server.
   For more information, see Restart the Endpoint Server.

Add a Mobile Collection License

On the License page in the Endpoint server, you can add a mobile collection license. You can also see information about an existing license for mobile collections.

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **License**.
   The License page appears.



3. Choose any of these actions under **Mobile License**.

Action	Steps
Add a mobile collection license.	Click **Add Mobile License** and then paste the license key into the **Add Mobile License** dialog box.
Review license information	Review this information: • the quantity of collection jobs remaining in the pool. • the date when the license expires.

Managing Settings

Administrators can complete these tasks on the Settings page in the Endpoint server web interface.

- Update Ports and Server Address
- Restart the Endpoint Server
- Create and Export an Agent Configuration File
- Update the Mobile Agent
- Set the Default Destination for Mobile Data Collections

Update Ports and Server Address

Before you begin, you should understand the information in the Default Server Ports topic.

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **Settings**.
   The Settings page appears.

3. Under **Server Ports**, update values in any of these fields as necessary.
   - Web Configuration Port
   - Agent Communication Port
   - Authentication Port
   - Server Address
4. Click **UPDATE**.
5. Restart the Endpoint server.
   For more information, see Restart the Endpoint Server.

Restart the Endpoint Server

You must restart the Endpoint server after you complete either of these tasks.

- Update the Endpoint Server License
- Update Ports and Server Address

There may be other occasions when it is necessary to restart the Endpoint server.

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **Settings**.
   The Settings page appears.

3. Scroll down to **Admin** and then click **RESTART SERVER**.

Create and Export an Agent Configuration File

This file (or the information in it) is required to configure Endpoint agents for remote computer collection.

Before you complete this task, verify that information on the Settings page under Server Ports is accurate. For more information, see Update Ports and Server Address.

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **Settings**.
   The Settings page appears.

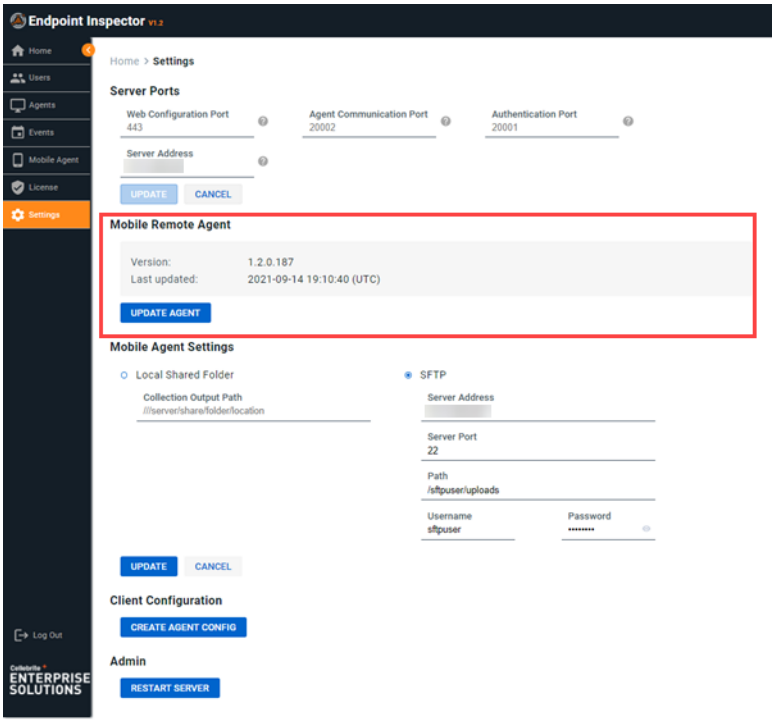
3. Scroll down to **Client Configuration** and then click **CREATE AGENT CONFIG**.
4. Save the resulting *config.json* file for distribution along with the installation files for the Endpoint agents.

Update the Mobile Agent

On the Settings page in the Endpoint server, you can see which version of the Endpoint mobile agent is in use and update to a new version of the mobile agent. You can get the most recent version from your account in the MyCellebrite portal.

This ensures that the newest version of the mobile agent is always used.

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **Settings**.
   The Settings page appears.



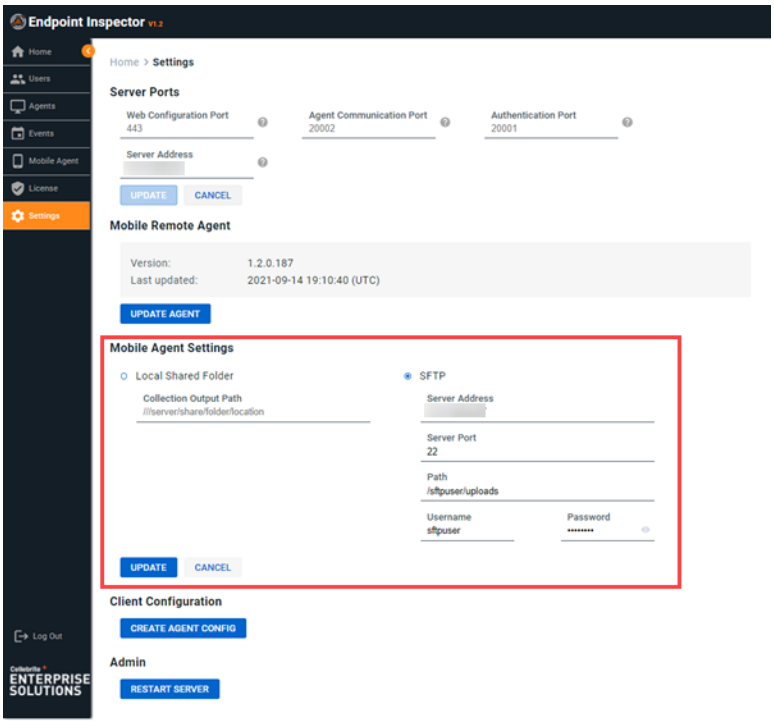
3. Under **Mobile Remote Agent**, review the **Version** and **Last updated** information to see which version is in use.
4. To get the most recent version of the Endpoint mobile agent, click **UPDATE AGENT**.
   The most recent version of the Endpoint mobile agent is downloaded to the computer in the destination you specify.
5. On the computer used as the Endpoint server, use File Explorer to browse to the downloaded Endpoint mobile agent and then open it.
   The mobile agent is uploaded to the Endpoint server.

Set the Default Destination for Mobile Data Collections

You can specify the default destination where mobile data collections will be saved. This should be a network location that is available to all custodians' computers. UNC and SFTP shares are supported.

For any individual collection job where the default destination is not appropriate, an examiner can specify an alternative destination.

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **Settings**.
   The Settings page appears.



3. Under **Mobile Agent Settings**, choose the appropriate option and provide the required information.

Option	Fields
Local Shared Folder	In **Collection Output Path**, type the file path for the network location for storing mobile data collections.
SFTP	Type the appropriate values in these fields. • **Server Address** • **Server Port** • **Path** • **Username** • **Password**

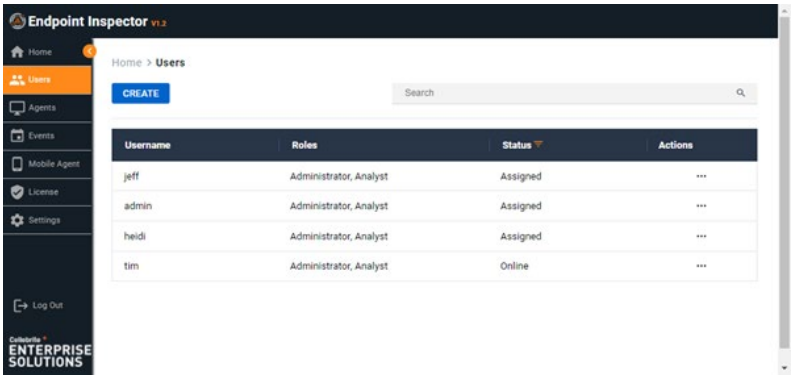
4. Click **UPDATE**.

Manage Users

Administrators can complete these tasks on the Users page in the Endpoint server web interface.

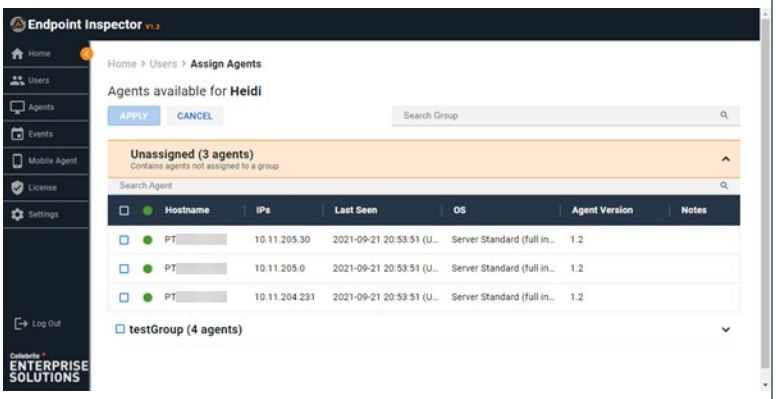
- Create users.
- Sort and filter the list of users.
- Delete users. You cannot delete yourself as a user.
- Update a user's password.
- Update a user's assigned roles. A user may have both or either the Administrator or Analyst roles assigned.
  - Users with only the Administrator role cannot have agents assigned.
  - Users with only the Analyst role cannot complete administrative tasks.
- For a user with the analyst role, assign or remove agents and groups of agents.

1. Log in to the web interface for your Endpoint server with administrative credentials
2. Click **Users**.
   The Users page appears.



3. Choose any of these actions.

Action	Steps
Create a user	1. Click **CREATE**. 2. Type the username and password. Usernames are not required to be email addresses. These characters are valid. • upper and lower-case letters • numerals 0-9 • @, dash, underbar, low dot 3. Assign either or both the Administrator and Analyst role. 4. Click **CREATE**.
Sort the list	Click a column label to toggle between ascending and descending order.

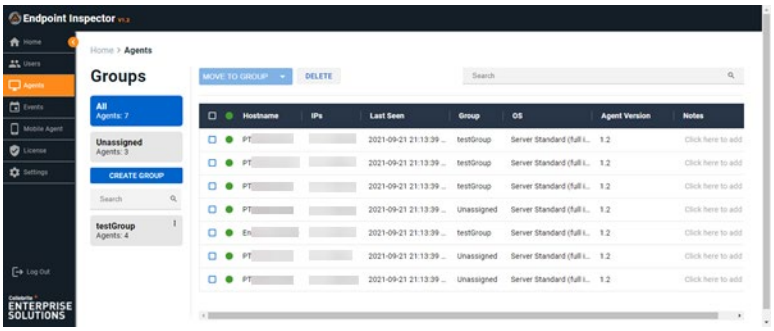
Action	Steps
Filter the list	Type anything in the **Search** box. The list of users is filtered on all columns based on what you typed.
Filter by column	Click (column filter) at the top of any column that has it, and then select the appropriate value. The list shows only those users that match.
Change a user's password or role	Find the appropriate user and then in the **Actions** column click **... (ellipsis) > Edit Profile.** • Change the password and then click **UPDATE PASSWORD**. • Change the assigned roles and then click **UPDATE ROLES**.
Copy text from a field	Right-click on the field you want to copy and then click **Copy Text**. The text from that field is copied to your clipboard.
Assign agents to a user	1. Find the appropriate user and then in the **Actions** column click **... (ellipsis) > Assign Agents**. The Assign Agents page appears.  2. Expand or collapse groups of agents, mark or unmark the checkboxes for the appropriate agent groups or individual agents, and then click **APPLY**.
Delete a user	Find the appropriate user and then in the **Actions** column click **... (ellipsis) > Delete**. You cannot delete yourself as a user.

Manage Agents and Groups

An Endpoint agent is created when it first connects successfully to the Endpoint server. Administrators can perform these tasks on the Agents page to manage agents and groups of agents.

- See the status of agents bound to this server for Endpoint Inspector.
- Search for agents and filter the list of agents. This filter is not case sensitive.
- Make a note for any agent. We recommend entering information to identify the person using this remote computer. This makes it easier for an examiner using Endpoint Inspector to choose Endpoint agents to connect to and collect files from.
- Create groups to more easily manage large amounts of agents and make it easier to assign agents to examiners. You can create groups in any way that makes sense for your organization. For example, you could group agents based on geography, such as Eastern, Central, and Western. Or you might group agents based on the platforms of the associated computers, or the departments those computers are in, such as Finance, Marketing, Executive, and so on.

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **Agents**.
   The Agents page appears.



   There are two default groups, All and Unassigned. All agents are always members of the All group.
3. Choose any of these actions.

Action	Steps
Sort the list of agents	Click a column label to toggle between ascending and descending order.
Filter the list	Type anything in the **Filter Groups** or **Filter Agents** box.
Copy from a field in the list	Right-click on the field you want to copy and then click **Copy Text**. The text from that field is copied to your clipboard.
Make a note for an agent	Find the appropriate agent and type in the **Notes** column.
Delete an agent	Mark the checkbox for the appropriate agent and then click **DELETE**.

Action	Steps
Create a group of agents	1. Click **CREATE GROUP**. 2. Type the name of the group and any notes about the group. 3. Assign appropriate agents to the group. 4. Click **CREATE**.
Move agents to a group	Select the appropriate agents and then click **MOVE TO GROUP**.
Filter the list of groups	Type anything in the **Search** box under CREATE GROUP. The list of groups is filtered based on what you typed.
See, edit, or delete a group	Select the group, click the ⋮ (vertical ellipsis) and then click **EDIT**. If you delete a group that has agents assigned, those agents become members of the Unassigned group.

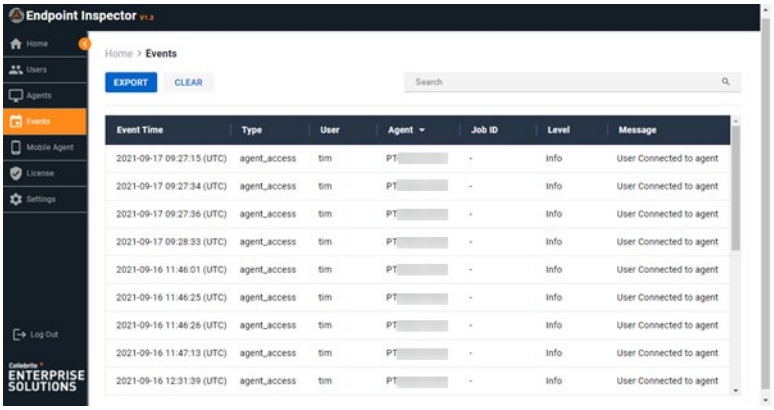
See the Event Log

On the Events page, administrators can export the event log to a .csv file. You may also clear events from the log.

These are some of the types of events you may see in the log.

- Examiners' attempts to log in to Endpoint Inspector (both successful and failed)
- Examiner access to Endpoint agents
- Mobile collection job events

1. Log in to the web interface for your Endpoint server with administrative credentials.
2. Click **Events**.
   The Events page appears.



3. Choose any of these actions.

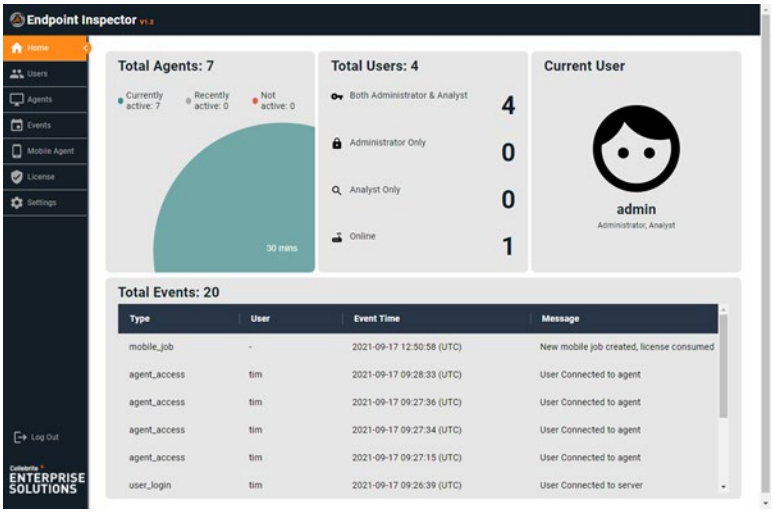
Action	Steps
Sort the list of events	Click a column label to toggle between ascending and descending order.
Filter the list of events	Type anything in the **Search** box. The list of events is filtered on all columns (except for Event Time and Job ID) based on what you type.
Copy from a field in the list	Right-click on the field you want to copy and then click **Copy Text**. The text from that field is copied to your clipboard.
Export the list of events	Click **EXPORT**. The list of events is saved according to the default settings for your web browser with the filename in this format: *endpoint_inspector_events_YYYY-MM-DDT_HH_MM_SS-timezone.csv.*
Clear the list of events	Click **CLEAR**. All events are removed from the log.

Review the Home Page

The Home page of the web interface for the Endpoint server shows a dashboard of status and activity information for agents and users associated with this server.

When you log in to the server or when you click **Home**, the Home page appears.

The Home page is refreshed every 30 seconds.



Total Agents shows the number of agents this server is managing. It also shows statistics about agent activity.

Total Users shows the total number of users this server is managing. It also shows statisticsabout users.

Total Events shows the total number of events logged since the list of events was last cleared. It also shows a list of the last ten events. You can sort this list by any column in ascending or descending order.

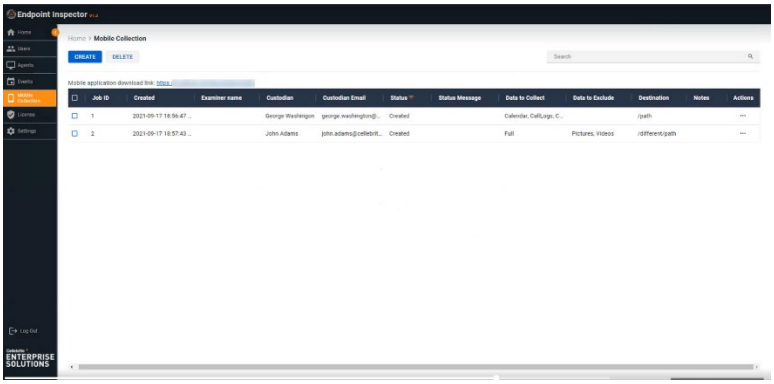
Examiner Tasks

Examiners can complete these tasks in the web interface for the Endpoint server.

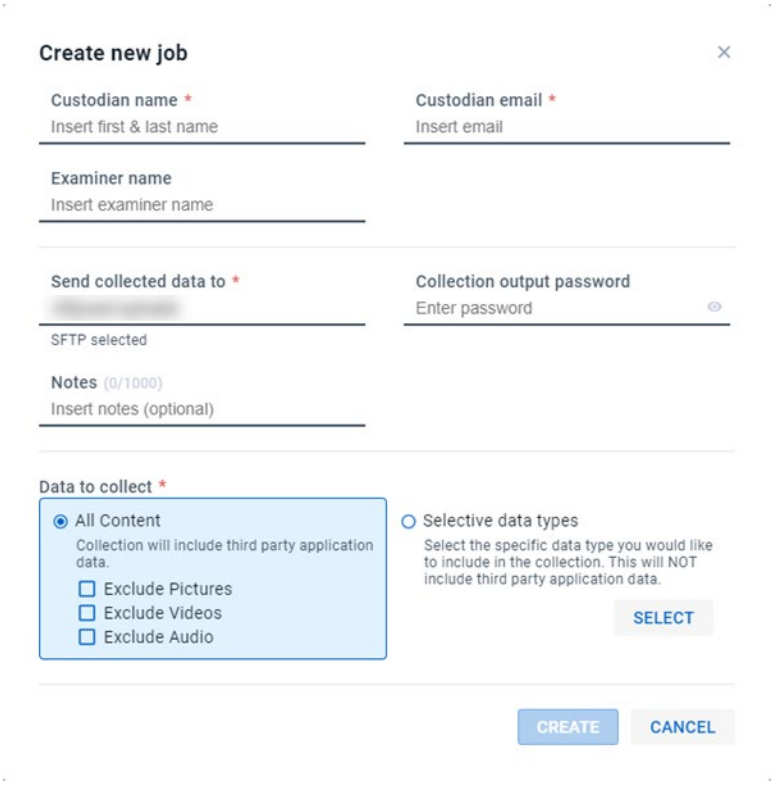
Create a Mobile Collection Job

A mobile collection job specifies what data to collect from a mobile agent and who the custodian of the mobile device is.

1. Use a web browser to log in to the web interface for your Endpoint server.
2. Click **Mobile Collection**.
   The Mobile Collection page appears.



3. Click **CREATE**.
   The Create new job page appears.



4. Type the appropriate information in these fields.

Field	Value
Custodian name	The full name of the custodian of the mobile device.
Custodian email	The email address of the custodian.
Examiner name	The name of the person who will examine the collected mobile data.
Send collected data to	If the default network location is not appropriate for this collection, type a different destination. This field is optional.
Collection output password	The password that will be required to open the mobile collection. This field is optional.
Notes	Any notes appropriate for this mobile collection job.

5. Under **Data to collect**, choose the appropriate option.
   - **All Content** collects data from all native and third-party applications supported by Endpoint Inspector. You may choose to exclude pictures, videos, or audio from the collection.

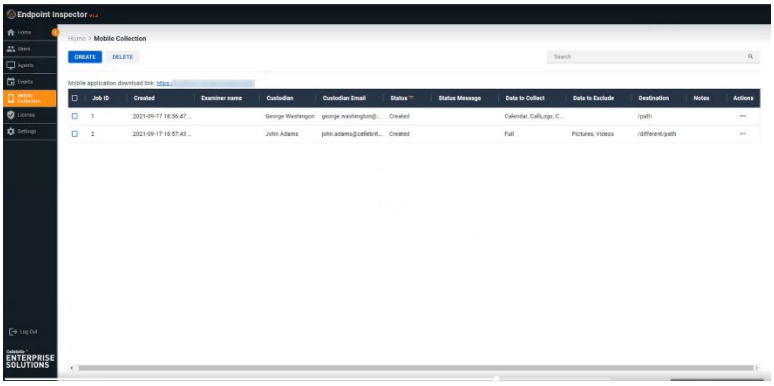
- **Selective data types** only collects data from native applications supported by Endpoint Inspector. It does not include third-party applications.
  Click **SELECT**, choose at least one data type to collect, and then click **CLOSE**. These are the data types you may select.
  - Select All
  - Advertising Identifier
  - Audio
  - Browser Data
  - Calendar
  - Call Logs
  - Contacts
  - Instant Messaging
  - Pictures
  - SMS/MMS
  - Videos

6. Click **CREATE**.
7. On the Mobile collection job created page, you can copy the activation token and the download link and paste them into the message the examiner will send to the custodian of the iOS device.

Send the Link and Activation Token to a Custodian

For each collection job, the examiner must provide the link and the activation token to the custodian, who uses these to start collection from the device in their custody. If you did not obtain the activation token and download link when the collection job was created, you can get them later.

1. Begin composing your message to the custodian.
2. Use a web browser to log in to the web interface for your Endpoint server.
3. Click **Mobile Collection**.
   The Mobile collection page appears.

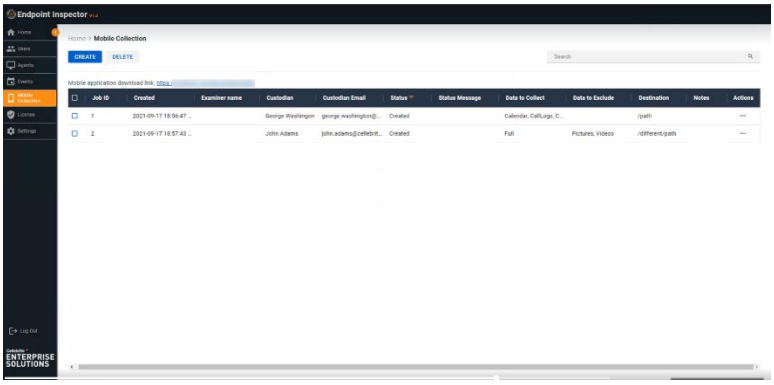


4. Above the list of agents, copy the link from where the mobile remote agent can be downloaded and paste it into your message to the custodian.
5. Find the appropriate collection job in the list, and then in the **Actions** column click **... (ellipsis) > Get Token.**
   The activation token is copied to your clipboard.
6. Paste the activation token into your message to the custodian.
7. Send the message to the custodian.

Monitor, Find, and Select Mobile Collection Jobs

Examiners can monitor the status of mobile collection jobs on the Mobile Collection page, which shows a list of all mobile collection jobs. You can see the status and details of each job as well as any status message. The status refreshes every 60 seconds.

1. Use a web browser to log in to the web interface for your Endpoint server.
2. Click **Mobile Collection**.
   The Mobile Collection page appears.



3. Choose the appropriate action.

Action	Steps
Sort by any column	Click a column label to toggle between ascending and descending order.
Show mobile collection jobs with a specific status	Click (column filter) at the top of the **Status** column and then select the appropriate status.
Filter the list	Type the appropriate information in the **Search** box. The list shows only mobile collection jobs that contain what you typed.
Copy from a field in the list	Right-click on the field you want to copy and then click **Copy Text**. The text from that field is copied to your clipboard.
Select a mobile collection job	Mark the checkbox to the left of the **Job ID** number.
Select all mobile collection jobs	Mark the checkbox to the left of the **Job ID** column title.

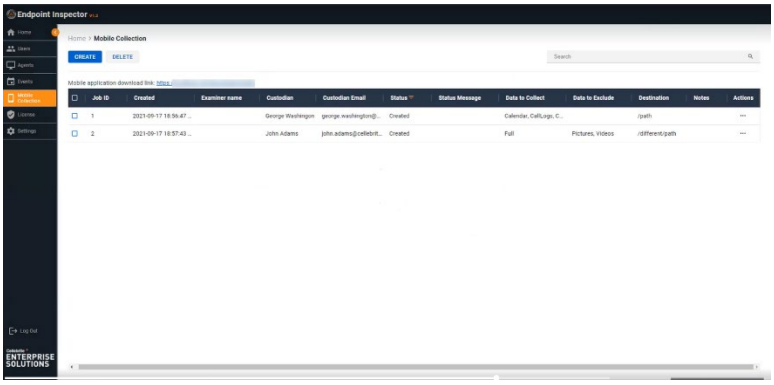
Delete a Mobile Collection Job

Examiners can delete a mobile collection job on the Mobile Collection page.

Deleting a collection job with a status of either Created or Extraction Failed returns it to the pool of available jobs. While you may delete mobile collection jobs with a different status, those jobs are consumed. Therefore, deleting them does not return them to the pool of available jobs.

Deleting a mobile collection job does not delete its stored data collection. Data collections related to deleted mobile collection jobs remain where they are stored until you manually move or delete them.

1. Use a web browser to log in to the web interface for your Endpoint server.
2. Click **Mobile Collection**.
   The Mobile Collection page appears.

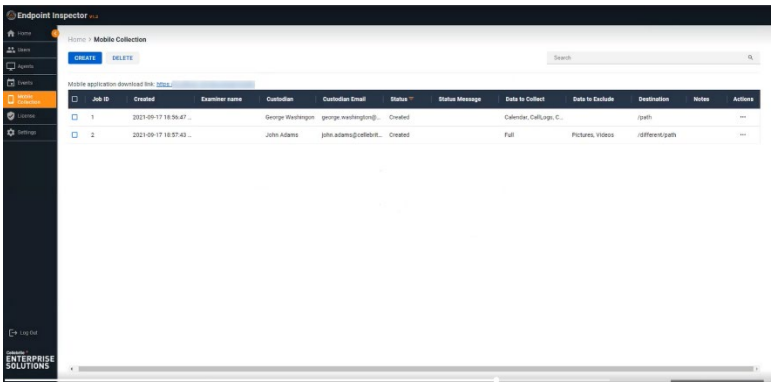


3. Select the appropriate mobile collection job and then click **DELETE**.

Get the Password for a Mobile Data Collection

Examiners can create a password for each collection job they create. If a password is created, it is required to open the collected data for examination. If you cannot recall the password for a collection job, you can see it on the Mobile Collection page.

1. Use a web browser to log in to the web interface for your Endpoint server.
2. Click **Mobile Collection**.
   The Mobile Collection page appears.



3. Find the appropriate collection job and then in the **Actions** column click **... (ellipsis) > Get Password.**
   The password is copied to your clipboard.

Troubleshooting

You may find this information helpful if you need to troubleshoot issues with mobile remote collections in Endpoint Inspector

- Closing Web Browser During Collection
- Log Files
  - Encrypted Session Log File
  - Other Log Files

Closing Web Browser During Collection

If the web browser on the custodian's computer is closed for more than 60 seconds during any part of the collection process, the mobile agent closes itself. The custodian must start the collection job again.

Log Files

Log files for mobile remote collection jobs are useful when you troubleshoot issues encountered by the custodian, such as the Endpoint mobile agent failing to run, to extract data, or to transmit the collected data. You can ask a custodian to send you any log files saved by the mobile agent on their computer.

Encrypted Session Log File

You should send the encrypted session log file to Cellebrite for investigation. The mobile agent automatically saves encrypted logs for each session in this folder:

%temp%\.Endpoint.Inspector.Extraction.Logs\<APP_START_TIME>

where %temp% is a windows shortcut to a temporary folder for the current user and <APP_START_TIME> is a folder with a name based on the time the mobile agent started in YYYY-MM-DD_HH-MM-SS format, for example:

C:\Users\<USER_NAME>\AppData\Local\Temp\.Endpoint.Inspector.Extraction.Logs\2021-08-12_14-01-36

Other Log Files

You can open these log files in any text editor, such as Notepad or TextEdit.

- If there are problems installing the mobile agent on the custodian's computer, you can set the installer for the mobile agent to save the log file by running the installer from the command line with this log parameter.

  `CellebriteMobileAgent_v<version number>.exe /log="LOG_FILE_PATH"`

  where <version number> is the version number in the name of the installation file for the mobile agent and "LOG_FILE_PATH" is the destination and file name for the log file, for example:

  `CellebriteMobileAgent _v1.2.0.191.exe /log="C:\<FOLDER_NAME>\LOG.TXT"`

  which is the full path and file name, or

  `CellebriteMobileAgent _v1.2.0.191.exe /log="LOG.TXT"`

  which creates the log file in the folder where the user is when they run this command.

- If the mobile agent user interface in the web browser shows something strange or does not respond to interaction, you can save logs from the web browser.

  1. Press F12 and then click **Console**.
  2. In the workspace, right-click to open the context menu and then click **Save As**.
  3. Save the log file with an appropriate name in an appropriate location.

Custodian Task

Custodians perform this mobile remote collection task.

- Create and Send a Mobile Collection

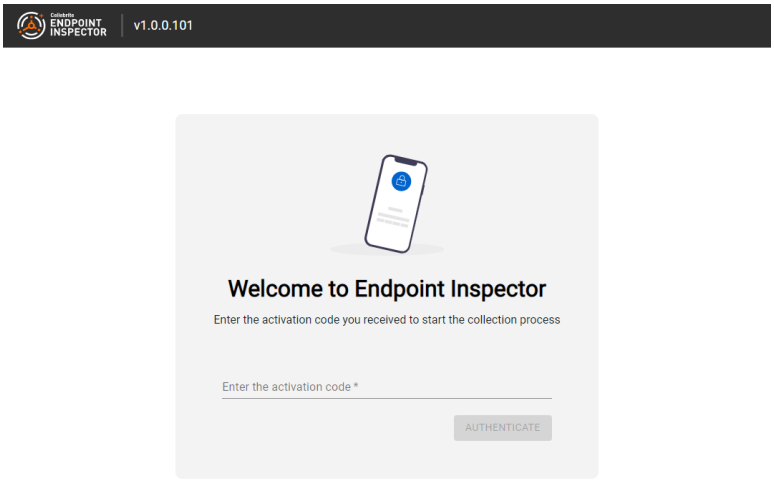
Create and Send a Mobile Collection

The custodian of the mobile device receives a message from the examiner. This message provides the link from which the Endpoint mobile agent is downloaded and installed onto the custodian's computer. The message also provides the activation token required to start collecting data.

Mobile remote collection is supported only for iOS devices.

Note: You must restart your computer after you install the Endpoint mobile agent. You must also have an appropriate USB cable to connect your mobile device to your computer when you are directed to do so.

1. On your computer, open the message and then click the link to download the installer for *Cellebrite.Mobile.Agent*.
2. Run the *Cellebrite.Mobile.Agent* installer and restart your computer.
3. Run the Cellebrite Endpoint Inspector mobile agent.
   The Welcome to Endpoint Inspector page appears in your web browser.



4. Paste the activation code from the message and then click **ACTIVATE**.
5. Follow the instructions provided in your web browser to connect your mobile device to your computer with an appropriate USB cable and disable automatic locking on your device.
   You may be required to provide a password for the device.
   If backup encryption is enabled, provide that password when you are directed to do so.
6. Follow the remaining instructions to collect the data and review the estimated time for the data collection to complete.
   The data collection is saved to your computer in the form of a single file.
7. When prompted on the Summary page, disconnect your mobile device from your computer and then click **NEXT**.

The data collection file is copied from your computer to the location specified by the examiner and then it is deleted from your computer. If your network connection is disrupted, transmission resumes automatically when the connection is reestablished.
If the data collection file cannot be sent to the destination specified by the examiner, this message appears: `Error sending data`.

a. To save the collection file to your computer, click **SAVE IN DIFFERENT LOCATION**.
b. Ask the examiner for instructions to manually send the collection file.